J. Symbolic Computation (2001) **31**, 259–276
doi:10.1006/jsco.1999.1015
Available online at http://www.idealibrary.com on IDEAL®

An Optimal Algorithm for Constructing the Reduced Gröbner Basis of Binomial Ideals, and Applications to Commutative Semigroups

ULLA KOPPENHAGEN† AND ERNST W. MAYR†

Institut für Informatik, Technische Universität München, D-80290 München, Germany

It is known that the reduced Gröbner basis of general polynomial ideals can be computed in exponential space. The algorithm, obtained by Kühnle and Mayr, is, however, based on rather complex parallel computations, and, above that, makes extensive use of the parallel computation thesis. In this paper, we exhibit an exponential space algorithm for generating the reduced Gröbner basis of binomial ideals which can be implemented without any complex parallel computations. This result is then applied to derive space optimal decision procedures for the finite enumeration and subword problems for commutative semigroups.

1. Introduction

The method of Gröbner bases (see Buchberger, 1965; also Hironaka, 1964) is a technique that provides algorithmic solutions to a variety of problems, for instance, primary decomposition of polynomial ideals, computations in the residue class ring modulo a polynomial ideal, decisions about various properties of ideals generated by a given finite set of polynomials, word problems modulo ideals and in commutative semigroups (reversible Petri nets), bijective enumeration of all polynomial ideals over a given coefficient domain etc.

Although versions of Buchberger's algorithm have been somewhat successful in practice, the complexity of the algorithm is not well understood. A first step in understanding the complexity of the algorithm is to bound the degree of polynomials that occur in a minimal Gröbner basis.

In the univariate case, the Gröbner-basis algorithm specializes to Euclid's algorithm whose complexity has been extensively studied (see Loos, 1982, for a survey). In the bivariate case Buchberger (1983) and Lazard (1983) gave important bounds on the degrees and the number of polynomials occurring in a reduced Gröbner basis. In the multivariate case, first steps towards an upper bound for the degrees in a minimal Gröbner basis were taken in Bayer (1982) and Möller and Mora (1984).

However, these results did not, or only under very restrictive assumptions, imply bounds for the degree of the polynomials arising during the intermediate computations of the Gröbner basis algorithms.

Using a novel partitioning method for polynomial ideals, Dubé (1990) obtained the

†E-mail: {koppenha|mayr}@in.tum.de, http://wwwmayr.informatik.tu-muenchen.de/

0747–7171/01/010259 + 18 $35.00/0

sharpened degree bound of $2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ (with d the maximum degree of the input basis and k the number of indeterminates) for the degree of polynomials in a reduced Gröbner basis, employing only combinatorial arguments.

An exponential bound on the degrees of Gröbner bases for zero-dimensional ideals was shown by Caniglia *et al.* (1988). Extending this result, Krick and Logar (1991) showed that Gröbner bases of zero- or one-dimensional ideals can be computed in time exponential in the number of indeterminates.

By transforming a representation of the normal form of a polynomial into a system of linear equations, Kühnle and Mayr (1996) exhibited an exponential space computation of Gröbner bases. This algorithm, however, is based on rather complex parallel computations like parallel rank computations of matrices, and, above that, makes extensive use of the parallel computation thesis (Fortune and Wyllie, 1978).

In this paper we present an exponential space algorithm for constructing the reduced Gröbner basis of a binomial ideal (each generator is a difference of two terms; for an investigation of the algebraic structure of binomial ideals see Eisenbud and Sturmfels, 1996). This algorithm can be implemented without any difficult parallel rank computations of matrices, or any other complex parallel computations. We make use of the close relationship between commutative semigroups and binomial ideals, in particular, of the algorithm in Mayr and Meyer (1982) for the uniform word problem in commutative semigroups. By the results in Mayr and Meyer (1982) and Huynh (1986), this algorithm is space optimal.

As applications of this algorithm we derive a procedure enumerating the elements of finite congruence classes in commutative semigroups and an algorithm for the general subword problem in commutative semigroups. Both algorithms use exponential space and are space optimal.

Another immediate application is computing complete rewrite systems for which we also obtain an exponential space completeness result (Huynh, 1986).

2. Basic Concepts and Notations

In this section we review some definitions and notations used in the following.

2.1. semigroups, Thue systems, and semigroup presentations

A *semigroup* $(H, \circ)$ is a set H with a binary operation $\circ$ which is associative. If additionally $\circ$ is commutative we have a *commutative semigroup*, and a semigroup with a unit element is called a *monoid*. For simplicity, we write ab instead of $a \circ b$.

A commutative monoid M is said to be *finitely generated* by a finite subset $X = \{x_1, \ldots, x_k\} \subseteq M$ if[†]

$$M = \{u | u = \underbrace{x_1 \ldots x_1}_{e_1} \underbrace{x_2 \ldots x_2}_{e_2} \ldots \underbrace{x_k \ldots x_k}_{e_k}, e_i \in \mathbb{N}, x_i \in X\}.$$

Each element of M can then be represented as a k-dimensional vector in $\mathbb{N}^k$, i.e. there is a surjection $\varphi : \mathbb{N}^k \to M$ such that

$$\varphi(e_1, \ldots, e_k) = \underbrace{x_1 \ldots x_1}_{e_1} \underbrace{x_2 \ldots x_2}_{e_2} \ldots \underbrace{x_k \ldots x_k}_{e_k}.$$

[†]$\mathbb{N}$ denotes the set of non-negative integers, and $\mathbb{Q}$ the set of rationals.

If φ is also injective, and hence bijective, then every element of M has a unique representation in $\mathbb{N}^k$, and M is said to be *free*.

For a finite alphabet $X = \{x_1, \ldots, x_k\}$, $X^\star$ denotes the free commutative monoid generated by X.

Let $\Phi : X^\star \to \mathbb{N}^k$ be the so-called Parikh mapping, i.e. $(\Phi(u))_i$ (also written $\Phi(u, x_i)$) indicates, for every $u \in X^\star$ and $i \in \{1, \ldots, k\}$, the number of occurrences of $x_i \in X$ in u.

For an element u of $X^\star$, called a (commutative) word, the order of the symbols is immaterial, and in the following we shall use an exponent notation: $u = x_1^{e_1} \ldots x_k^{e_k}$, where $e_i = \Phi(u, x_i) \in \mathbb{N}$ for $i = 1, \ldots, k$.

A *commutative semi-Thue system* over X is given by a finite set $\mathcal{P}$ of productions $l_i \to r_i$, where $l_i, r_i \in X^\star$. A word $v \in X^\star$ *is derived in one step* from $u \in X^\star$ (written $u \to v(\mathcal{P})$) by application of the production $(l_i \to r_i) \in \mathcal{P}$ iff, for some $w \in X^\star$, we have $u = wl_i$ and $v = wr_i$. The word u *derives* v iff $u \xrightarrow{*} v(\mathcal{P})$, where $\xrightarrow{*}$ is the reflexive transitive closure of $\to$. More precisely we write $u \xrightarrow{+} v(\mathcal{P})$, where $\xrightarrow{+}$ is the transitive closure of $\to$, if $u \xrightarrow{*} v(\mathcal{P})$ and $u \neq v$. A sequence $(u_0, \ldots, u_n)$ of words $u_i \in X^\star$ with $u_i \to u_{i+1}(\mathcal{P})$ for $i = 0, \ldots, n-1$ is called a *derivation* (of length n) of u_n from u_0 in $\mathcal{P}$.

A *commutative Thue system* is a symmetric commutative semi-Thue system $\mathcal{P}$, i.e.

$$(l \to r) \in \mathcal{P} \Rightarrow (r \to l) \in \mathcal{P}.$$

Derivability in a commutative Thue system establishes a congruence $\equiv_{\mathcal{P}}$ on $X^\star$ by the rule

$$u \equiv v \bmod \mathcal{P} \Leftrightarrow_{def} u \xrightarrow{*} v(\mathcal{P}).$$

Thus, for commutative Thue systems, we also use the notation $l \equiv r \bmod \mathcal{P}$ to denote the pair of productions $(l \to r)$ and $(r \to l)$ in $\mathcal{P}$.

A commutative Thue system $\mathcal{P}$ is also called a *presentation of the commutative quotient semigroup* $X^\star / \equiv_{\mathcal{P}}$.

We note that commutative semi-Thue systems appear in other, equivalent formulations in the literature, like *vector addition systems* and *Petri nets*. Finitely presented commutative semigroups are equivalent to *reversible* vector addition systems or Petri nets. Readers more familiar with reversible Petri nets may want to think of a vector in $\mathbb{N}^k$ as a marking.

2.2. POLYNOMIALS AND IDEALS

Let X denote the finite set $\{x_1, \ldots, x_k\}$, and $\mathbb{Q}[X]$ the (commutative) ring of polynomials with indeterminates $x_1, \ldots, x_k$ and rational coefficients. A *term* t in $x_1, \ldots, x_k$ is a product of the form $t = x_1^{e_1} \cdot x_2^{e_2} \cdots x_k^{e_k}$, with $e = (e_1, e_2, \ldots, e_k) \in \mathbb{N}^k$ the *degree vector* of t. By the *degree* $\deg(t)$ of a term t we shall mean the integer $e_1 + e_2 + \cdots + e_k$ (which is ≥ 0). Each *polynomial* $f(x_1, \ldots, x_k) \in \mathbb{Q}[X]$ is a finite sum $f(x_1, \ldots, x_k) = \sum_{i=1}^{n} a_i \cdot t_i$, with $a_i \in \mathbb{Q} - \{0\}$ the coefficient of the ith term t_i of f. The product $m_i = a_i \cdot t_i$ is called the ith *monomial* of the polynomial f. The degree of a polynomial is the maximum of the degrees of its terms.

An *ideal* in $\mathbb{Q}[X]$ is any subset I of $\mathbb{Q}[X]$ satisfying the following conditions:

(I1) $\quad p, q \in I \quad \Rightarrow \quad p + q \in I;$

(I2) $\quad r \in \mathbb{Q}[X], p \in I \quad \Rightarrow \quad r \cdot p \in I.$

For $f_1, \ldots, f_h \in \mathbb{Q}[X]$, $\langle f_1, \ldots, f_h \rangle \subseteq \mathbb{Q}[X]$ denotes the ideal generated by $\{f_1, \ldots, f_h\}$,

that is[†]

$$\langle f_1, \ldots, f_h \rangle := \left\{ \sum_{i=1}^{h} p_i f_i;\ p_i \in \mathbb{Q}[X] \quad \text{for} \quad i \in I_h \right\}.$$

If $I = \langle f_1, \ldots, f_h \rangle$, $\{f_1, \ldots, f_h\}$ is called a *basis* of I.

An *admissible term ordering* $\prec$ on $\mathbb{Q}[X]$ is given by any admissible order on $\mathbb{N}^k$, i.e. any total order $<$ on $\mathbb{N}^k$ satisfying the following two conditions:

(T1) $e > (0, \ldots, 0)$ for all $e \in \mathbb{N}^k - \{(0, \ldots, 0)\}$;

(T2) $a < b \quad \Rightarrow \quad a + c < b + c$ for all $a, b, c \in \mathbb{N}^k$.

If $(d_1, \ldots, d_k) > (e_1, \ldots, e_k)$, we say that any monomial $a_1 \cdot x_1^{d_1} \cdots x_k^{d_k}$, $a_1 \in \mathbb{Q} - \{0\}$, *is greater* in the term ordering than any monomial $a_2 \cdot x_1^{e_1} \cdots x_k^{e_k}$, $a_2 \in \mathbb{Q} - \{0\}$ (written $a_1 \cdot x_1^{d_1} \cdots x_k^{d_k} \succ a_2 \cdot x_1^{e_1} \cdots x_k^{e_k}$).

For a polynomial $f(x_1, \ldots, x_k) = \sum_{i=1}^{n} a_i \cdot t_i$ we always assume that $t_1 \succ t_2 \succ \cdots \succ t_n$. For any such non-zero polynomial $f \in \mathbb{Q}[X]$ we define the *leading term* $LT(f) := t_1$.

For the sake of constructiveness, we assume that the term ordering is given as part of the input by a $k \times k$ integer matrix T such that $a_1 \cdot x_1^{d_1} \cdots x_k^{d_k} \succ a_2 \cdot x_1^{e_1} \cdots x_k^{e_k}$ iff, for the corresponding degree vectors d and e, Td is *lexicographically greater* than Te (see Robbiano, 1985; Weispfenning, 1987)

Let I be an ideal in $\mathbb{Q}[X]$, and let some admissible term ordering $\prec$ on $\mathbb{Q}[X]$ be given. A finite set $\{g_1, \ldots, g_r\}$ of polynomials from $\mathbb{Q}[X]$ is called a *Gröbner* basis of I (w.r.t. $\prec$), if

(G1) $\{g_1, \ldots, g_r\}$ is a basis of I;

(G2) $\{LT(g_1), \ldots, LT(g_r)\}$ is a basis of the *leading term ideal* of I, which is the smallest ideal $\subseteq \mathbb{Q}[X]$ containing the leading terms of all $f \in I$, or equivalently: if $f \in I$, then $\quad LT(f) \in \langle LT(g_1), \ldots, LT(g_r) \rangle$.

A Gröbner basis is called *reduced* if no monomial in any one of its polynomials is divisible by the leading term of any other polynomial in the basis.

3. The Connection between Commutative Semigroups and Binomial Ideals

3.1. The basic problems and their relationship

In this section, we consider the *uniform word problem* for commutative semigroups and the *polynomial ideal membership problem*. We will show the relationship between these two very basic and fundamental algorithmic problems for commutative semigroups and polynomial ideals.

Let $\mathcal{P} = \{l_i \equiv r_i;\ i \in I_h\}$ be some (finite) commutative semigroup presentation with l_i, $r_i \in X^\star$ for $i \in I_h$. We identify any $u \in X^\star$ (resp. the corresponding vector $u = (\Phi(u, x_1), \ldots, \Phi(u, x_k)) \in \mathbb{N}^k$) with the term $u = x_1^{\Phi(u,x_1)} \cdot x_2^{\Phi(u,x_2)} \cdots x_k^{\Phi(u,x_k)}$ and vice versa any term $u = x_1^{e_1} \cdot x_2^{e_2} \cdots x_k^{e_k} \in \mathbb{Q}[X]$ with the word

$$u = \underbrace{x_1 \ldots x_1}_{e_1} \underbrace{x_2 \ldots x_2}_{e_2} \ldots \underbrace{x_k \ldots x_k}_{e_k} \in X^\star.$$

[†]For $n \in \mathbb{N}$, I_n denotes the set $\{1, \ldots, n\}$.

By $I(\mathcal{P})$ we denote the $\mathbb{Q}[X]$-ideal generated by $\{l_1 - r_1, \ldots, l_h - r_h\}$, i.e.

$$I(\mathcal{P}) := \left\{ \sum_{i=1}^{h} p_i(l_i - r_i);\ p_i \in \mathbb{Q}[X] \text{ for } i \in I_h \right\}.$$

We call such an ideal a *binomial ideal*, i.e. each polynomial in the basis is the difference of two terms. By looking at Buchberger's (1965) algorithm it is not hard to see that the reduced Gröbner basis of a binomial ideal still consists only of binomials.

The *Uniform Word Problem* for commutative semigroups is: Given a commutative semigroup presentation $\mathcal{P}$ over some alphabet X, and two words $u, v \in X^\star$, decide whether $u \equiv v \bmod \mathcal{P}$.

The *Polynomial Ideal Membership Problem* is: Given polynomials $f, f_1, \ldots, f_h \in \mathbb{Q}[X]$, decide whether $f \in \langle f_1, \ldots, f_h \rangle$.

Proposition 3.1. (Mayr and Meyer, 1982) *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^\star, i \in I_h\}$, and u, $v \in X^\star$. Then the following are equivalent:*

(i) *there exist $p_1, \ldots, p_h \in \mathbb{Q}[X]$ such that* $v - u = \sum_{i=1}^{h} p_i(l_i - r_i)$;

(ii) *there is a derivation $u = \gamma_1 \to \gamma_2 \to \ldots \to \gamma_n = v(\mathcal{P})$ of v from u in $\mathcal{P}$ such that for $j \in I_n$* $\deg(\gamma_j) \leq \max\{\deg(l_i p_i), \deg(r_i p_i);\ i \in I_h\}$;

(iii) $u \equiv v \bmod \mathcal{P}$.

In the fundamental paper (Hermann, 1926), G. Hermann gave a doubly exponential degree bound for the polynomial ideal membership problem:

Proposition 3.2. (Hermann, 1926) *Let $X = \{x_1, \ldots, x_k\}$, $g, g_1, \ldots, g_h \in \mathbb{Q}[X]$, and $d := \max\{\deg(g_i);\ i \in I_h\}$. If $g \in \langle g_1, \ldots, g_h \rangle$, then there exist $p_1, \ldots, p_h \in \mathbb{Q}[X]$ such that*

(i) $g = \sum_{i=1}^{h} g_i p_i$;

(ii) $(\forall i \in I_h);\ [\deg(p_i) \leq \deg(g) + (hd)^{2^k}]$.

By size$(\cdot)$ we shall denote the number of bits needed to encode the argument in some standard way (using radix representation for numbers).

Then the above two propositions yield an exponential space upper bound for the uniform word problem for commutative semigroups:

Proposition 3.3. (Mayr and Meyer, 1982) *Let $X = \{x_1, \ldots, x_k\}$ and $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^\star, i \in I_h\}$. Then there is a (deterministic) Turing machine M and some constant $c > 0$ independent of $\mathcal{P}$, such that M decides for any two words u, $v \in X^\star$ whether $u \equiv v \bmod \mathcal{P}$ using at most space* $(\text{size}(u, v, \mathcal{P}))^2 \cdot 2^{c \cdot k}$.

3.2. the reduced Gröbner basis for binomial ideals

Let $\mathcal{P}$ be a commutative semigroup presentation over some alphabet X, and $\prec$ some admissible term ordering on $\mathbb{Q}[X]$. The following two theorems characterize the binomials of the reduced Gröbner basis of $I(\mathcal{P})$ (w.r.t. $\prec$). The first shows that in each binomial of

the reduced Gröbner basis G of $I(\mathcal{P})$ the smaller term (w.r.t. $\prec$) is the minimal element (w.r.t. $\prec$) of the congruence class of the leading term.

THEOREM 3.1. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^\star, i \in I_h\}$, and $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ be the reduced Gröbner basis of the ideal $I(\mathcal{P})$ w.r.t. some admissible term ordering $\prec$ ($m_i \prec h_i$). Then m_i is the minimal element (w.r.t. $\prec$) of the congruence class $[h_i]_\mathcal{P}$, $i \in I_r$.*

PROOF. Assume that $w \neq m_i$ is the minimal element of $[h_i]_\mathcal{P}$ (w.r.t. $\prec$). Then $w \prec m_i$ and $m_i - w \in I(\mathcal{P})$. Since G is a Gröbner basis of $I(\mathcal{P})$, $m_i \in \langle h_1, \ldots, h_r\rangle$, i.e. there must be some $j \in I_r$ such that h_j divides m_i. This however contradicts the fact that $h_i - m_i$ is an element of the reduced Gröbner basis of $I(\mathcal{P})$.□

The next theorem characterizes the leading terms of the polynomials in $I(\mathcal{P})$.

THEOREM 3.2. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^\star, i \in I_h\}$, and $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ be the reduced Gröbner basis of the ideal $I(\mathcal{P})$ w.r.t. some admissible term ordering $\prec$ ($m_i \prec h_i$). Then $LT(I(\mathcal{P}))$ (the set of the leading terms of $I(\mathcal{P})$) is the set of all terms with non-trivial congruence class which are* not *the minimal element in their congruence class w.r.t. $\prec$. $H = \{h_1, \ldots, h_r\}$ is the set of the minimal elements of $LT(I(\mathcal{P}))$ w.r.t. divisibility.*

PROOF. Since G is the reduced Gröbner basis of $I(\mathcal{P})$, it is clear that H is the set of the minimal elements of $LT(I(\mathcal{P}))$ w.r.t. divisibility.

Since $h_i - m_i \in I(\mathcal{P})$, there is a derivation in $\mathcal{P}$ of $m_i \prec h_i$ from h_i ($h_i \xrightarrow{+} m_i(\mathcal{P})$), for all $i \in I_r$. Because G is a Gröbner basis, for any $h \in LT(I(\mathcal{P}))$ there is an $h_j - m_j \in G$ and a term t in X with $h = t \cdot h_j$ and $h \xrightarrow{+} t \cdot m_j(\mathcal{P})$. Thus, for any $h \in LT(I(\mathcal{P}))$, the congruence class $[h]_\mathcal{P}$ is non-trivial, and h is not the minimal element in $[h]_\mathcal{P}$.

Let $s \in X^\star$ be a term with non-trivial congruence class. If s is not the minimal element m_s (w.r.t. $\prec$) of its congruence class $[s]_\mathcal{P}$, then s derives m_s ($s \xrightarrow{+} m_s(\mathcal{P})$), and thus, $s - m_s \in I(\mathcal{P})$, i.e. $s \in LT(I(\mathcal{P}))$. If $s = m_s$, then there is no derivation of any $t_s \prec s$ from s, and there is no $h_j \in H$ such that h_j divides s. This is because if there is some $h_j \in H$ and some term t in X with $s = t \cdot h_j$, then $s \equiv t \cdot m_j \bmod \mathcal{P}$ what contradicts the minimality of s. Thus, if $s = m_s$, then $s \notin LT(I(\mathcal{P}))$ and $s \notin H$.□

4. An Optimal Algorithm for the Reduced Gröbner Basis

In this section we give an exponential space algorithm for generating the reduced Gröbner basis of a binomial ideal. To determine the complexity of the algorithm we need the results of Section 3 and the following upper bound for the total degree of polynomials required in a Gröbner basis, obtained by Dubé (1990). Note that we use exponential notation in representing words over X.

PROPOSITION 4.1. (DUBÉ, 1990) *Let $X = \{x_1, \ldots, x_k\}$, $F = \{f_1, \ldots, f_h\} \subset \mathbb{Q}[X]$, $I = \langle f_1, \ldots, f_h\rangle$ the ideal generated by F, and let d be the maximum degree of any $f \in F$. Then, for any admissible term ordering $\prec$ on $\mathbb{Q}[X]$, the degree of polynomials required in a Gröbner basis for I w.r.t. $\prec$ is bounded by $2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$.*

Now we will generate the reduced Gröbner basis of the binomial ideal $I(\mathcal{P})$ w.r.t. some fixed admissible term ordering $\prec$, where $X = \{x_1, \ldots, x_k\}$ and $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^\star, i \in I_h\}$ (w.l.o.g. $l_i \succ r_i$). Let H denote the set $\{h_1, \ldots, h_r\}$ of the minimal elements of $LT(I(\mathcal{P}))$ w.r.t. divisibility, and m_i the minimal element of $[h_i]_\mathcal{P}$ w.r.t. $\prec$, for $i \in I_r$. From Theorems 3.1 and 3.2 we know that the set $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ is the reduced Gröbner basis of $I(\mathcal{P})$.

We have to determine the elements in H, as well as the minimal element m_i (w.r.t. $\prec$) of the congruence class of each $h_i \in H$. From Proposition 4.1 we know that the degrees $\deg(h_i)$ and $\deg(m_i)$ are bounded by $2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, where d is the maximum degree of any $l_i - r_i$, $i \in I_h$.

LEMMA 4.1. *For a term $u \in X^\star$ with non-trivial congruence class the minimal element w.r.t. $\prec$ of $[u]_\mathcal{P}$ is of the form $t \cdot r_i$ with $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^\star$.*

PROOF. W.l.o.g. assume that u is not the minimal element m_u of $[u]_\mathcal{P}$ w.r.t. $\prec$. Then there is a derivation in $\mathcal{P}$ leading from u to $m_u \prec u$, i.e. $u \xrightarrow{+} m_u(\mathcal{P})$, where $m_u = t \cdot r_i$ for some $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^\star$ (note that $l_j \succ r_j\ \forall j \in I_h$).□

For $h = x_1^{e_1} \cdots x_k^{e_k} \in X^\star$ and $i \in I_k$ such that $e_i \geq 1$, define $h^{(i)} := x_1^{e_1} \cdots x_i^{e_i - 1} \cdots x_k^{e_k}$. Then H consists exactly of those terms $h \in X^\star$ which have degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, which are congruent to some term $t \cdot r_i \prec h$ with $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^\star$, and $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, and for which, for all applicable i, $[h^{(i)}]_\mathcal{P}$ is trivial. By Proposition 3.3, the condition regarding the reducibility of h can be checked in space $(\text{size}(\mathcal{P}))^2 \cdot 2^{c \cdot k}$ for some constant $c > 0$ independent of $\mathcal{P}$. Testing non-reducibility of the $h^{(i)}$ can also be done in exponential space because of Proposition 3.3 and:

LEMMA 4.2. *A term $u \in X^\star$ with $\deg(u) \leq D$ is an element of $LT(I(\mathcal{P}))$ iff there is some $t \cdot r_i$ with $t \cdot r_i \prec u$, $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^\star$, and $\deg(t \cdot r_i) \leq D + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ such that $u \xrightarrow{+} t \cdot r_i(\mathcal{P})$.*

PROOF. We only have to prove the degree bound. Note that $u \in LT(I(\mathcal{P}))$ iff either $u \in H$, and thus $\deg(m_u) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$, where m_u is the minimal element of $[u]_\mathcal{P}$, or there is some $h \in H$ with $u = t_u \cdot h$ for some $t_u \in X^\star$. The degree of the minimal element m_h of $[h]_\mathcal{P}$ w.r.t. $\prec$ is bounded by $2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$. From $m_h \prec h$ we get $t_u \cdot m_h \prec u$ with $\deg(t_u \cdot m_h) \leq D + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$.□

From this, we derive the exponential space algorithm given in Figure 1.

Putting everything together, we have proven the following theorem.

THEOREM 4.1. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^\star, i \in I_h\}$, and $\prec$ some admissible term ordering. Then there is an algorithm which generates the reduced Gröbner basis $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ of the binomial ideal $I(\mathcal{P})$ using at most space $(\text{size}(\mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k} \leq 2^{c \cdot \text{size}(\mathcal{P})}$, where $\bar{c}, c > 0$ are some constants independent of $\mathcal{P}$.*

The Algorithm

Input: admissible term ordering $\prec$, $\mathcal{P} = \{l_1 - r_1, \ldots, l_h - r_h\}$ with $r_i \prec l_i \; \forall i \in I_h$
Output: the reduced Gröbner basis $G = \{h_1 - m_1, \ldots, h_r - m_r\}$ of $I(\mathcal{P})$

$d := \max\{\deg(l_i),\ \deg(r_i);\ i \in I_h\}$
$G := \emptyset$

for each $h = x_1^{e_1} \cdots x_k^{e_k} \in X^\star$ with degree $\leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ **do**
  $gb :=$ **false**
  if there exists $t \cdot r_i$ with $t \cdot r_i \prec h$, $r_i \in \{r_1, \ldots, r_h\}$, $t \in X^\star$, $\deg(t \cdot r_i) \leq 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$
    which is $\equiv h \bmod \mathcal{P}$ **then** /* $h \in LT(I(\mathcal{P}))$ */
    $m :=$ the minimal (w.r.t. $\prec$) among these terms
    $gb :=$ **true**
  end_if
  $D := \deg(h)$
  for each $i \in I_k$ with $e_i \geq 1$ **while** gb **do**
    $h' := x_1^{e_1} \cdots x_i^{e_i - 1} \cdots x_k^{e_k}$
    if there exists $t \cdot r_j$ with $t \cdot r_j \prec h'$, $r_j \in \{r_1, \ldots, r_h\}$, $t \in X^\star$, $\deg(t \cdot r_j) \leq$
      $(D-1) + 2 \cdot \left(\frac{d^2}{2} + d\right)^{2^{k-1}}$ which is $\equiv h' \bmod \mathcal{P}$ **then**
      /* $h' \in LT(I(\mathcal{P})) \Rightarrow h \notin H$ */
      $gb :=$ **false**
    end_if
  end_for
  if gb **then** /* $h \in H$ */
    $G := G \cup \{h - m\}$
  end_if
end_for

Figure 1. Algorithm for constructing the reduced Gröbner basis of a binomial ideal.

From the results in Huynh (1986) we know that, in the worst case, any Gröbner basis of $I(\mathcal{P})$ has maximal degree at least $2^{2^{c' \cdot \mathrm{size}(\mathcal{P})}}$ for some constant $c' > 0$ independent of $\mathcal{P}$. Hence, any algorithm that computes Gröbner bases of binomial ideals requires at least exponential space in the worst case.

5. Applications

We now consider two applications of the exponential space algorithm obtained in Section 4. We present space optimal decision procedures for the finite enumeration and subword problems for commutative semigroups.

5.1. The finite enumeration problem for commutative semigroups

Let $\mathcal{P}$ be a finite commutative semigroup presentation over some alphabet X, and $u \in X^\star$ a word such that the congruence class of u is finite (or, synonymously, *bounded*). Then the finite enumeration problem for commutative semigroups, or equivalently, reversible

Petri nets is the problem of generating a complete list of all the elements of $[u]_{\mathcal{P}}$. We give a procedure for the solution of this problem which needs at most exponential work space.

THEOREM 5.1. *Let $X = \{x_1, \ldots, x_k\}$, $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^\star, i \in I_h\}$ be a finite commutative semigroup presentation over X, and $u \in X^\star$ a word such that the congruence class of u is finite. Then there is an algorithm which generates the elements of $[u]_{\mathcal{P}}$ using at most space $(\mathrm{size}(u,\mathcal{P}))^2 \cdot 2^{\bar{c}\cdot k} \leq 2^{c\cdot \mathrm{size}(u,\mathcal{P})}$, where $\bar{c}$, $c > 0$ are some constants independent of u and $\mathcal{P}$.*

PROOF. In addition to $x_1, \ldots, x_k$ we introduce $2k+3$ new variables m, s, t, $y_1, \ldots, y_k$ and $z_1, \ldots, z_k$. Let $X' = X \cup \{m, s, t, y_1, \ldots, y_k, z_1, \ldots, z_k\}$. Given $\mathcal{P}$ and the word $u \in X^\star$, we construct a new commutative semigroup presentation $\mathcal{P}'$ over X' as follows: $\mathcal{P}'$ contains the relations

$$s \cdot x_j \equiv s \cdot y_j \cdot z_j, \qquad \text{for} \quad j = 1, \ldots, k, \tag{5.1}$$

$$s \cdot y(u) \equiv t, \tag{5.2}$$

$$s \cdot u \equiv m, \tag{5.3}$$

and, for every relation $l_i \equiv r_i$ in $\mathcal{P}$, the relation

$$s \cdot y(l_i) \equiv s \cdot y(r_i), \quad \text{and} \tag{5.4}$$

$$t \cdot z(l_i) \equiv t \cdot z(r_i), \tag{5.5}$$

where y, resp. z are the homomorphisms replacing x_j by y_j, resp. z_j, $j \in I_k$.

Let $\prec$ be a lexicographic term ordering satisfying

$$m \prec a \prec s \prec b \qquad \text{for all} \quad a \in \{x_1, \ldots, x_k\}, b \in \{t, y_1, \ldots, y_k, z_1, \ldots, z_k\}.$$

In the following we prove that $v \in [u]_{\mathcal{P}}$ iff $s \cdot v - m \in G$, where G is the reduced Gröbner basis of the ideal $I(\mathcal{P}')$ w.r.t. $\prec$. Then, by Theorem 4.1, the elements of $[u]_{\mathcal{P}}$ can be generated using at most space $(\mathrm{size}(u,\mathcal{P}'))^2 \cdot 2^{d'\cdot k} \leq (\mathrm{size}(u,\mathcal{P}))^2 \cdot 2^{d\cdot k}$, where d', $d > 0$ are some constants independent of u and $\mathcal{P}'$, resp. $\mathcal{P}$.

First we establish some technical details.

LEMMA 5.1. *Every word $w \in [s \cdot u]_{\mathcal{P}'}$ satisfies the following conditions:*

(i) $\Phi(w,s) + \Phi(w,t) + \Phi(w,m) = 1$;

(ii) *if* $\Phi(w,s) = 1$, *then* $x_1^{\Phi(w,x_1)+\Phi(w,y_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,y_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,y_k)} \in [u]_{\mathcal{P}}$,

$$x_1^{\Phi(w,x_1)+\Phi(w,z_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,z_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,z_k)} \in [u]_{\mathcal{P}};$$

if $\Phi(w,t) = 1$, *then* $\Phi(w,x_1) = \Phi(w,x_2) = \ldots = \Phi(w,x_k) = 0$,

$$\Phi(w,y_1) = \Phi(w,y_2) = \ldots = \Phi(w,y_k) = 0,$$

$$x_1^{\Phi(w,z_1)} \cdot x_2^{\Phi(w,z_2)} \cdots x_k^{\Phi(w,z_k)} \in [u]_{\mathcal{P}}.$$

PROOF. Let w be any word in $[s \cdot u]_{\mathcal{P}'}$. Then there is a repetition-free derivation in $\mathcal{P}'$ leading from $s \cdot u$ to w. If $w = m$, then w is derived in one step from $s \cdot u$ by relation (5.3) and w trivially satisfies conditions (i) and (ii). Note that if in a derivation starting at $s \cdot u$ relation (5.3) is applied, then this derivation can only be continued by again using

relation (5.3), causing a repetition. If $w \neq m$, then in any repetition-free derivation starting at $s \cdot u$ leading to w only the relations in (5.1) and (5.4) can be applied until the word $s \cdot y(u) \cdot z(u)$ is reached and changed to $t \cdot z(u)$ by relation (5.2). Since $[u]_{\mathcal{P}}$ is finite, there is no $u' \in \{y_1, \ldots, y_k\}^\star$ with $s \cdot u' \cdot z(u) \in [s \cdot u]_{\mathcal{P}'}$, $u' \neq y(u)$, and $y(u)$ divides u'. Therefore, any word w occurring in this derivation of $s \cdot y(u) \cdot z(u)$ from $s \cdot u$ satisfies conditions (i) and (ii):

(i) $\Phi(w, s) = 1$, $\Phi(w, t) = 0$, $\Phi(w, m) = 0$,

(ii) $x_1^{\Phi(w,x_1)+\Phi(w,y_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,y_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,y_k)} \in [u]_{\mathcal{P}}$, and

$$x_1^{\Phi(w,x_1)+\Phi(w,z_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,z_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,z_k)} = u.$$

Then, as long as relation (5.2) is not applied, by the relations in (5.5), words $t \cdot z(v)$ with $v \in [u]_{\mathcal{P}}$ can be derived from $t \cdot z(u)$. Note that for all such words $t \cdot z(v)$ with $v \in [u]_{\mathcal{P}}$ $\Phi(t \cdot z(v), s) = 0$, $\Phi(t \cdot z(v), t) = 1$, $\Phi(t \cdot z(v), m) = 0$, and condition (ii) is satisfied. Relation (5.2) changes $t \cdot z(v)$ to $s \cdot y(u) \cdot z(v)$ and again the relations in (5.1) and (5.4) can be applied. As above, the words w in the resulting sub-derivation starting at $s \cdot y(u) \cdot z(v)$ satisfy (i) and (ii) with

$$x_1^{\Phi(w,x_1)+\Phi(w,z_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,z_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,z_k)} = v.$$

By the relations in (5.4), from $s \cdot y(u) \cdot z(v)$ any word $s \cdot y(v') \cdot z(v)$ with $v' \in [u]_{\mathcal{P}}$ can be derived. Relation (5.2) can only be applied to the word $s \cdot y(u) \cdot z(v)$, causing a repetition. Thus, conditions (i) and (ii) are satisfied within the whole derivation. This completes the proof of Lemma 5.1.□

For the derivation of some word $s \cdot v \in [s \cdot u]_{\mathcal{P}'}$, with $v \in X^\star$, from $s \cdot u$ in $\mathcal{P}'$ we conclude from Lemma 5.1 and its proof:

Corollary 5.1. *Let $s \cdot v \in [s \cdot u]_{\mathcal{P}'}$ with $v \in X^\star$, $v \neq u$, and let $s \cdot u = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_n = s \cdot v$ be any repetition-free derivation in $\mathcal{P}'$ leading from $s \cdot u$ to $s \cdot v$. Then there is exactly one $i \in I_{n-1}$ with $\gamma_i = s \cdot y(u) \cdot z(u)$, $\gamma_{i+1} = t \cdot z(u)$, and exactly one $j \in I_{n-1}$, $j > i$, with $\gamma_j = t \cdot z(v)$, $\gamma_{j+1} = s \cdot y(u) \cdot z(v)$.*

Thus, we can prove:

Lemma 5.2. *Let v be some word in $X^\star$, then*

$$v \in [u]_{\mathcal{P}} \quad \Longleftrightarrow \quad s \cdot v \in [s \cdot u]_{\mathcal{P}'}.$$

Proof. By Lemma 5.1 and its Corollary 5.1, a repetition-free derivation in $\mathcal{P}'$ leading from $s \cdot u$ to $s \cdot v$ with $v \in X^\star$ has the following form:

$$s \cdot u \xrightarrow[(5.1),(5.4)]{+} s \cdot y(u) \cdot z(u) \xrightarrow{(5.2)} t \cdot z(u) \xrightarrow[(5.5)]{+} t \cdot z(v) \xrightarrow{(5.2)} s \cdot y(u) \cdot z(v) \xrightarrow[(5.1),\,(5.4)]{+} s \cdot v,$$

where $\xrightarrow[(.)]{+}$ denotes some repetition-free derivation applying only the relations given in (.). Within the sub-derivations $\xrightarrow[(5.1),\,(5.4)]{+}$, the values $\Phi(w, x_i) + \Phi(w, z_i)$ are constant

for all $i \in I_k$, i.e. the word $x_1^{\Phi(w,x_1)+\Phi(w,z_1)} \cdot x_2^{\Phi(w,x_2)+\Phi(w,z_2)} \cdots x_k^{\Phi(w,x_k)+\Phi(w,z_k)}$ remains the same within $\overset{+}{\underset{(5.1),\,(5.4)}{\longrightarrow}}$. Furthermore, all words occurring in the above derivation satisfy Lemma 5.1.□

LEMMA 5.3. *$[s \cdot u]_{\mathcal{P}'}$ is finite.*

PROOF. Since $[u]_{\mathcal{P}}$ is finite, it follows from the definition of $\mathcal{P}'$ and Lemma 5.1 that $[s \cdot u]_{\mathcal{P}'}$ is also finite.□

LEMMA 5.4. *Let v be some word in $X^\star$ with $v \notin [u]_{\mathcal{P}}$, and v divides some $u' \in [u]_{\mathcal{P}}$. Then $s \cdot v$ is the minimal (w.r.t. $\prec$) element of its congruence class $[s \cdot v]_{\mathcal{P}'}$.*

PROOF. If $v \in X^\star$ with $v \notin [u]_{\mathcal{P}}$, and v divides some $u' \in [u]_{\mathcal{P}}$, then there is some $v' \in X^\star - \{\varepsilon\}$ with $u' = v \cdot v' \in [u]_{\mathcal{P}}$. Because of the finiteness of $[u]_{\mathcal{P}}$ there is no $\bar{v} \in [v]_{\mathcal{P}}$ with $\bar{v} = u \cdot \bar{u}$ for $\bar{u} \in X^\star$. If there is such a $\bar{v} \in [v]_{\mathcal{P}}$, then $u' = v \cdot v' \equiv \bar{v} \cdot v' \bmod \mathcal{P}$, $\bar{v} \cdot v' = u \cdot \bar{u} \cdot v' \in [u]_{\mathcal{P}}$, i.e. $[u]_{\mathcal{P}}$ is not finite. Thus, in any derivation starting at $s \cdot v$ relations (5.2) and (5.3) cannot be applied. Only the relations in (5.1) and (5.4) can possibly be used. Since $y_i \succ x_i$ (resp. $z_i \succ x_i$) for all $i \in I_k$, $s \cdot v$ is the minimal element of $[s \cdot v]_{\mathcal{P}'}$ w.r.t. $\prec$.□

Note that each $v \in X^\star$ is the minimal (w.r.t. $\prec$) element of $[v]_{\mathcal{P}'}$ because no relation in $\mathcal{P}'$ is applicable.

Since $[s \cdot u]_{\mathcal{P}'}$ is finite, it follows from Dickson's (1913) Lemma that each $w \in [s \cdot u]_{\mathcal{P}'}$ is minimal in $[s \cdot u]_{\mathcal{P}'}$ w.r.t. divisibility, i.e. if $w \in [s \cdot u]_{\mathcal{P}'}$, then there is no $w' \in [s \cdot u]_{\mathcal{P}'}$, $w' \neq w$ such that w' divides w. The minimal element w.r.t. $\prec$ of $[s \cdot u]_{\mathcal{P}'}$ is m. Thus, by Lemma 5.4, each $s \cdot v \in [s \cdot u]_{\mathcal{P}'}$ with $v \in X^\star$ is contained in the set of the minimal elements of $LT(I(\mathcal{P}'))$ w.r.t. divisibility, and hence $G \supseteq \{s \cdot v - m \mid s \cdot v \in [s \cdot u]_{\mathcal{P}'}, v \in X^\star\}$ (see Theorems 3.1 and 3.2). This establishes Theorem 5.1.□

As an example of Theorem 5.1, consider the finite commutative semigroup presentation $\mathcal{P} = \{x_1^2 \equiv x_1 x_2^3, x_2^2 \equiv x_2 x_3^3\}$ over the alphabet $X = \{x_1, x_2, x_3\}$ and the word $u = x_1^3$. Splitting each relation of $\mathcal{P}$ into its two corresponding productions provides

$$x_1^2 \to x_1 x_2^3, \tag{5.1}$$
$$x_1 x_2^3 \to x_1^2, \tag{5.2}$$
$$x_2^2 \to x_2 x_3^3, \tag{5.3}$$
$$x_2 x_3^3 \to x_2^2. \tag{5.4}$$

Applying these productions, the congruence class $[u]_{\mathcal{P}}$ of u in $\mathcal{P}$ can be derived as shown in Figure 2 ($v_1 \xrightarrow{(.)} v_2$ means that v_2 is derived in one step from v_1 by application of production (.)). Note that $[u]_{\mathcal{P}}$ is finite.

Using the construction of Theorem 5.1 we compute the reduced Gröbner basis G of the ideal

$$I := \langle sy_1z_1 - sx_1, sy_2z_2 - sx_2, sy_3z_3 - sx_3,$$

$$
\begin{array}{lccccccc}
[u]_{\mathcal{P}}\colon\ u = x_1^3 & \underset{(5.2)}{\overset{(5.1)}{\rightleftarrows}} & x_1^2x_2^3 & \underset{(5.2)}{\overset{(5.1)}{\rightleftarrows}} & x_1x_2^6 & & & \\
 & & (5.3)\downarrow\uparrow(5.4) & & (5.3)\downarrow\uparrow(5.4) & & & \\
 & & x_1^2x_2^2x_3^3 & \underset{(5.2)}{\overset{(5.1)}{\rightleftarrows}} & x_1x_2^5x_3^3 & & & \\
 & & (5.3)\downarrow\uparrow(5.4) & & (5.3)\downarrow\uparrow(5.4) & & & \\
 & & x_1^2x_2x_3^6 & \underset{(5.2)}{\overset{(5.1)}{\rightleftarrows}} & x_1x_2^4x_3^6 & & & \\
 & & & & (5.3)\downarrow\uparrow(5.4) & & & \\
 & & & & x_1x_2^3x_3^9 & \underset{(5.1)}{\overset{(5.2)}{\rightleftarrows}} & x_1^2x_3^9 & \\
 & & & & (5.3)\downarrow\uparrow(5.4) & & & \\
 & & & & x_1x_2^2x_3^{12} & & & \\
 & & & & (5.3)\downarrow\uparrow(5.4) & & & \\
 & & & & x_1x_2x_3^{15} & & &
\end{array}
$$

Figure 2. Deriving the congruence class $[u]_{\mathcal{P}}$.

$$sy_1^2 - sy_1y_2^3, sy_2^2 - sy_2y_3^3, tz_1^2 - tz_1z_2^3, tz_2^2 - tz_2z_3^3,$$
$$t - sy_1^3, sx_1^3 - m\rangle$$

w.r.t. the lexicographic term ordering $\succ$ satisfying

$$t \succ z_1 \succ z_2 \succ z_3 \succ y_1 \succ y_2 \succ y_3 \succ s \succ x_1 \succ x_2 \succ x_3 \succ m.$$

The result is given in Figure 3. By making a comparison with Figure 2 one can verify that

$$v \in [u]_{\mathcal{P}} \qquad \text{iff} \quad s \cdot v - m \in G.$$

THEOREM 5.2. *The finite enumeration problem for commutative semigroups is exponential space complete with respect to log–lin reducibility.*

From the work in Mayr and Meyer (1982) we know that the uniform word problem for commutative semigroups is exponential space complete (the input consisting of u, v and $\mathcal{P}$). Actually, the construction in Mayr and Meyer (1982) proves the following, slightly stronger statement, which we will use for the proof of Theorem 5.2:

PROPOSITION 5.1. (MAYR AND MEYER, 1982) *Let $\mathcal{P}$ be a finite commutative semigroup presentation over some alphabet X, v a word in $X^\star$, and $u \in X^\star$ a word such that $[u]_{\mathcal{P}}$ is finite. Even with this restriction, the uniform word problem,* i.e. *the problem of deciding whether $u \equiv v \bmod \mathcal{P}$, is exponential space complete with respect to log–lin reducibility.*

PROOF OF THEOREM 5.2. Let $\mathcal{P}$ be the commutative semigroup presentation, and u, $v \in X^\star$ the two words of Proposition 5.1. Then $v \equiv u \bmod \mathcal{P}$, i.e. $v \in [u]_{\mathcal{P}}$ iff v is

$$
\begin{aligned}
sx_1x_2x_3^{15} &- m\\
sx_1x_2^2x_3^{12} &- m\\
sx_1x_2^3x_3^9 &- m\\
sx_1x_2^4x_3^6 &- m\\
sx_1x_2^5x_3^3 &- m\\
sx_1x_2^6 &- m\\
sx_1^2x_3^9 &- m\\
sx_1^2x_2x_3^6 &- m\\
sx_1^2x_2^2x_3^3 &- m\\
sx_1^2x_2^3 &- m\\
sx_1^3 &- m\\
x_2m &- x_3^3m\\
x_1m &- x_3^9m\\
sx_3^{27}m &- m^2\\
y_3sx_1x_2^2x_3^{11} &- y_3sx_1x_2x_3^{14}\\
y_3sx_1x_2^3x_3^8 &- y_3sx_1x_2x_3^{14}\\
y_3sx_1x_2^4x_3^5 &- y_3sx_1x_2x_3^{14}\\
y_3sx_1x_2^5x_3^2 &- y_3sx_1x_2x_3^{14}\\
y_3sx_1^2x_3^8 &- y_3sx_1x_2x_3^{14}\\
y_3sx_1^2x_2x_3^5 &- y_3sx_1x_2x_3^{14}\\
y_3sx_1^2x_2^2x_3^2 &- y_3sx_1x_2x_3^{14}\\
y_3^2sx_1x_2^2x_3^{10} &- y_3^2sx_1x_2x_3^{13}\\
y_3^2sx_1x_2^3x_3^7 &- y_3^2sx_1x_2x_3^{13}\\
y_3^2sx_1x_2^4x_3^4 &- y_3^2sx_1x_2x_3^{13}\\
y_3^2sx_1x_2^5x_3 &- y_3^2sx_1x_2x_3^{13}\\
y_3^2sx_1^2x_3^7 &- y_3^2sx_1x_2x_3^{13}\\
y_3^2sx_1^2x_2x_3^4 &- y_3^2sx_1x_2x_3^{13}\\
y_3^2sx_1^2x_2^2x_3 &- y_3^2sx_1x_2x_3^{13}\\
y_3^3sx_1x_2^2x_3^9 &- y_3^3sx_1x_2x_3^{12}\\
y_3^3sx_1x_2^3x_3^6 &- y_3^3sx_1x_2x_3^{12}\\
y_3^3sx_1x_2^4x_3^3 &- y_3^3sx_1x_2x_3^{12}\\
y_3^3sx_1x_2^5 &- y_3^3sx_1x_2x_3^{12}\\
y_3^3sx_1^2x_3^6 &- y_3^3sx_1x_2x_3^{12}\\
y_3^3sx_1^2x_2x_3^3 &- y_3^3sx_1x_2x_3^{12}\\
y_3^3sx_1^2x_2^2 &- y_3^3sx_1x_2x_3^{12}\\
y_3^4sx_1x_2^2x_3^8 &- y_3^4sx_1x_2x_3^{11}\\
y_3^4sx_1x_2^3x_3^5 &- y_3^4sx_1x_2x_3^{11}\\
y_3^4sx_1x_2^4x_3^2 &- y_3^4sx_1x_2x_3^{11}\\
y_3^4sx_1^2x_3^5 &- y_3^4sx_1x_2x_3^{11}\\
y_3^4sx_1^2x_2x_3^2 &- y_3^4sx_1x_2x_3^{11}\\
y_3^5sx_1x_2^2x_3^7 &- y_3^5sx_1x_2x_3^{10}\\
y_3^5sx_1x_2^3x_3^4 &- y_3^5sx_1x_2x_3^{10}\\
y_3^5sx_1x_2^4x_3 &- y_3^5sx_1x_2x_3^{10}\\
y_3^5sx_1^2x_3^4 &- y_3^5sx_1x_2x_3^{10}\\
y_3^5sx_1^2x_2x_3 &- y_3^5sx_1x_2x_3^{10}\\
y_3^6sx_1x_2^2x_3^6 &- y_3^6sx_1x_2x_3^9\\
y_3^6sx_1x_2^3x_3^3 &- y_3^6sx_1x_2x_3^9\\
y_3^6sx_1x_2^4 &- y_3^6sx_1x_2x_3^9\\
y_3^6sx_1^2x_3^3 &- y_3^6sx_1x_2x_3^9\\
y_3^6sx_1^2x_2 &- y_3^6sx_1x_2x_3^9\\
y_3^7sx_1x_2^2x_3^5 &- y_3^7sx_1x_2x_3^8\\
y_3^7sx_1x_2^3x_3^2 &- y_3^7sx_1x_2x_3^8\\
y_3^7sx_1^2x_3^2 &- y_3^7sx_1x_2x_3^8\\
y_3^8sx_1x_2^2x_3^4 &- y_3^8sx_1x_2x_3^7\\
y_3^8sx_1x_2^3x_3 &- y_3^8sx_1x_2x_3^7\\
y_3^8sx_1^2x_3 &- y_3^8sx_1x_2x_3^7\\
y_3^9sx_1x_2^2x_3^3 &- y_3^9sx_1x_2x_3^6\\
y_3^9sx_1x_2^3 &- y_3^9sx_1x_2x_3^6\\
y_3^9sx_1^2 &- y_3^9sx_1x_2x_3^6\\
y_3^{10}sx_1x_2^2x_3^2 &- y_3^{10}sx_1x_2x_3^5\\
y_3^{11}sx_1x_2^2x_3 &- y_3^{11}sx_1x_2x_3^4\\
y_3^{12}sx_1x_2^2 &- y_3^{12}sx_1x_2x_3^3\\
y_2m &- y_3^3m\\
y_2sx_2 &- y_3^3sx_2\\
y_2sx_1^2 &- y_3^3sx_1^2\\
y_2^2s &- y_2y_3^3s\\
y_1m &- y_3^9m\\
y_1sx_2^2x_3^{12} &- y_1sx_2x_3^{15}\\
y_1sx_2^3x_3^9 &- y_1sx_2x_3^{15}\\
y_1sx_2^4x_3^6 &- y_1sx_2x_3^{15}\\
y_1sx_2^5x_3^3 &- y_1sx_2x_3^{15}\\
y_1sx_2^6 &- y_1sx_2x_3^{15}\\
y_1sx_1 &- y_2y_3^6sx_1\\
y_1y_3sx_2^2x_3^{11} &- y_1y_3sx_2x_3^{14}\\
y_1y_3sx_2^3x_3^8 &- y_1y_3sx_2x_3^{14}\\
y_1y_3sx_2^4x_3^5 &- y_1y_3sx_2x_3^{14}\\
y_1y_3sx_2^5x_3^2 &- y_1y_3sx_2x_3^{14}\\
y_1y_3^2sx_2^2x_3^{10} &- y_1y_3^2sx_2x_3^{13}\\
y_1y_3^2sx_2^3x_3^7 &- y_1y_3^2sx_2x_3^{13}\\
y_1y_3^2sx_2^4x_3^4 &- y_1y_3^2sx_2x_3^{13}\\
y_1y_3^2sx_2^5x_3 &- y_1y_3^2sx_2x_3^{13}\\
y_1y_3^3sx_2^2x_3^9 &- y_1y_3^3sx_2x_3^{12}\\
y_1y_3^3sx_2^3x_3^6 &- y_1y_3^3sx_2x_3^{12}\\
y_1y_3^3sx_2^4x_3^3 &- y_1y_3^3sx_2x_3^{12}\\
y_1y_3^3sx_2^5 &- y_1y_3^3sx_2x_3^{12}\\
y_1y_3^4sx_2^2x_3^8 &- y_1y_3^4sx_2x_3^{11}\\
y_1y_3^4sx_2^3x_3^5 &- y_1y_3^4sx_2x_3^{11}\\
y_1y_3^4sx_2^4x_3^2 &- y_1y_3^4sx_2x_3^{11}\\
y_1y_3^5sx_2^2x_3^7 &- y_1y_3^5sx_2x_3^{10}\\
y_1y_3^5sx_2^3x_3^4 &- y_1y_3^5sx_2x_3^{10}\\
y_1y_3^5sx_2^4x_3 &- y_1y_3^5sx_2x_3^{10}\\
y_1y_3^6sx_2^2x_3^6 &- y_1y_3^6sx_2x_3^9\\
y_1y_3^6sx_2^3x_3^3 &- y_1y_3^6sx_2x_3^9\\
y_1y_3^6sx_2^4 &- y_1y_3^6sx_2x_3^9\\
y_1y_3^7sx_2^2x_3^5 &- y_1y_3^7sx_2x_3^8\\
y_1y_3^7sx_2^3x_3^2 &- y_1y_3^7sx_2x_3^8\\
y_1y_3^8sx_2^2x_3^4 &- y_1y_3^8sx_2x_3^7\\
y_1y_3^8sx_2^3x_3 &- y_1y_3^8sx_2x_3^7\\
y_1y_3^9sx_2^2x_3^3 &- y_1y_3^9sx_2x_3^6\\
y_1y_3^9sx_2^3 &- y_1y_3^9sx_2x_3^6\\
y_1y_3^{10}sx_2^2x_3^2 &- y_1y_3^{10}sx_2x_3^5\\
y_1y_3^{11}sx_2^2x_3 &- y_1y_3^{11}sx_2x_3^4\\
y_1y_3^{12}sx_2^2 &- y_1y_3^{12}sx_2x_3^3\\
y_1^2s &- y_1y_2y_3^6s\\
z_3y_3m &- x_3m\\
z_3y_3s &- sx_3\\
z_2m &- z_3^3m\\
z_2sx_2x_3^3 &- z_3^3sx_2^2\\
z_2sx_1^2x_3^3 &- z_3^3sx_1^2x_2\\
z_2y_3sx_2x_3^2 &- z_3^2sx_2^2\\
z_2y_3sx_1^2x_3^2 &- z_3^2sx_1^2x_2\\
z_2y_3^2sx_2x_3 &- z_3sx_2^2\\
z_2y_3^2sx_1^2x_3 &- z_3sx_1^2x_2\\
z_2y_3^3sx_2 &- sx_2^2\\
z_2y_3^3sx_1^2 &- sx_1^2x_2\\
z_2y_2s &- sx_2\\
z_1m &- z_3^9m\\
z_1sx_1x_2x_3^6 &- z_2z_3^6sx_1^2\\
z_1sx_1x_2^2x_3^3 &- z_2^2z_3^3sx_1^2\\
z_1sx_1x_2^3 &- z_2^3sx_1^2\\
z_1y_3sx_1x_2x_3^5 &- z_2z_3^5sx_1^2\\
z_1y_3sx_1x_2^2x_3^2 &- z_2^2z_3^2sx_1^2\\
z_1y_3^2sx_1x_2x_3^4 &- z_2z_3^4sx_1^2\\
z_1y_3^2sx_1x_2^2x_3 &- z_2^2z_3sx_1^2\\
z_1y_3^3sx_1x_2x_3^3 &- z_2z_3^3sx_1^2\\
z_1y_3^3sx_1x_2^2 &- z_2^2sx_1^2\\
z_1y_3^4sx_1x_2x_3^2 &- z_2z_3^2sx_1^2\\
z_1y_3^5sx_1x_2x_3 &- z_2z_3sx_1^2\\
z_1y_3^6sx_1x_2 &- z_2sx_1^2\\
z_1y_2sx_1x_3^6 &- z_3^6sx_1^2\\
z_1y_2y_3sx_1x_3^5 &- z_3^5sx_1^2\\
z_1y_2y_3^2sx_1x_3^4 &- z_3^4sx_1^2\\
z_1y_2y_3^3sx_1x_3^3 &- z_3^3sx_1^2\\
z_1y_2y_3^4sx_1x_3^2 &- z_3^2sx_1^2\\
z_1y_2y_3^5sx_1x_3 &- z_3sx_1^2\\
z_1y_2y_3^6sx_1 &- sx_1^2\\
z_1y_1s &- sx_1\\
t &- y_1y_2y_3^{15}s
\end{aligned}
$$

Figure 3. The reduced Gröbner basis of the binomial ideal I.

contained in the list of elements of $[u]_{\mathcal{P}}$ generated by the enumeration algorithm of Theorem 5.1. Thus, an exponential space complete word problem reduces to the finite enumeration problem for commutative semigroups, which together with Theorem 5.1

establishes the exponential space completeness of the finite enumeration problem for commutative semigroups.□

5.2. THE SUBWORD PROBLEM FOR COMMUTATIVE SEMIGROUPS

Let $X = \{x_1, \ldots, x_k\}$ be a finite alphabet, and $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^\star, i \in I_h\}$ a finite commutative semigroup presentation over X.

The (ordinary) subword problem for commutative semigroups is to decide, for any two words u, $v_1 \in X^\star$, whether there is a $v_2 \in [u]_\mathcal{P}$ such that $v_2 = v_1 \cdot w$ for some $w \in X^\star$ which contains no variable occurring in v_1. In other words, if such a word v_2 exists, then w.l.o.g. the variables can be renamed such that

$$v_2 = \underbrace{x_1^{e_1} \cdots x_a^{e_a}}_{v_1} \cdot \underbrace{x_{a+1}^{e_{a+1}} \cdots x_k^{e_k}}_{w},$$

for some $e_1, \ldots, e_a \in \mathbb{N} - \{0\}$ and $e_{a+1}, \ldots, e_k \in \mathbb{N}$.

By X_{v_1} we denote the set of variables occurring in v_1, i.e. $v_1 \in X_{v_1}^\star$ and $\Phi(v_1, x_i) > 0$ for all $x_i \in X_{v_1}$. If $X_{v_1} \neq X$, then we denote by $X_{\overline{v_1}}$ the set of variables not occurring in v_1, i.e. $X_{\overline{v_1}} = X \setminus X_{v_1}$.

Let Y, Z be subsets of X with $Y \cap Z = \emptyset$.

W.l.o.g. the variables can be renamed such that $X_{v_1} = \{x_1, \ldots, x_a\}$, $X_{\overline{v_1}} = \{x_{a+1}, \ldots, x_k\}$, $Y = \{x_{a_1}, x_{a_1+1}, \ldots, x_{a_2}\}$ (if $a_1 > a_2$, then $Y = \emptyset$) and $Z = \{x_1, \ldots, x_{a_0}\} \cup \{x_{a_3}, \ldots, x_k\}$ (if $1 > a_0$ and $k < a_3$, then $Z = \emptyset$). Then, for the case $1 < a_0 < a_1 < a < a_2 < a_3 < k$, we get the following picture:

$$\overbrace{\underbrace{x_1, \ldots, x_{a_0}}_{Z}, x_{a_0+1}, \ldots, x_{a_1-1}, \underbrace{x_{a_1}, \ldots, x_a}_{Y}}^{X_{v_1}}, \overbrace{\underbrace{x_{a+1}, \ldots, x_{a_2}}_{Y}, x_{a_2+1}, \ldots, x_{a_3-1}, \underbrace{x_{a_3}, \ldots, x_k}_{Z}}^{X_{\overline{v_1}}}.$$

With this notation we define the subword, word, and coverability problems for commutative semigroups as follows. Note that the definition of the subword problem extends the definition given at the beginning of this section.

- The *Subword Problem* is: Given X, $\mathcal{P}$, u, v_1, Y and Z, decide whether there is a $v_2 \in [u]_\mathcal{P}$ such that $v_2 = v_1 \cdot x_{a_1} \cdots x_{a_2} \cdot w$ for some $w \in (Y \cup Z)^\star$ if $a_1 \leq a_2$, resp. $v_2 = v_1 \cdot w$ for some $w \in Z^\star$ if $a_1 > a_2$.
- The *Word Problem* is: Given X, $\mathcal{P}$, u, v_1, decide whether $v_1 \in [u]_\mathcal{P}$. (In Mayr and Meyer (1982) this problem has been shown to be exponential space complete.)
- The *Coverability Problem* is: Given X, $\mathcal{P}$, u, v_1, decide whether there is a $v_2 \in [u]_\mathcal{P}$ such that v_1 is a subword of v_2, i.e. $v_2 = v_1 \cdot w$ for some $w \in X^\star$. (In Koppenhagen and Mayr (1995) we have shown that this problem is exponential space complete.)

We observe that the word problem and the coverability problem are special cases of the subword problem. If Y and Z are both empty, then the subword problem is equivalent to the word problem. If Y is empty and $Z = X$, then the subword problem is equivalent to the coverability problem.

If Y is empty and $Z = X_{\overline{v_1}}$, we get the former definition. Then the subword problem is to decide whether there is a $v_2 \in [u]_\mathcal{P}$ such that $v_2 = v_1 \cdot w$ for some $w \in X_{\overline{v_1}}^\star$.

THEOREM 5.3. *Let $X = \{x_1, \ldots, x_k\}$ and $\mathcal{P} = \{l_i \equiv r_i;\ l_i, r_i \in X^\star, i \in I_h\}$ be a finite commutative semigroup presentation over X. Then there is an algorithm which, for any two words u, $v_1 \in X^\star$, and sets $Y \subseteq X$, $Z \subseteq X \setminus Y$, decides whether there is, and if so, also provides a $v_2 \in [u]_\mathcal{P}$ such that $v_2 = v_1 \cdot v \cdot w$, where $w \in (Y \cup Z)^\star$ and $v = x_{a_1} \cdots x_{a_2}$ if $Y = \{x_{a_1}, x_{a_1+1}, \ldots, x_{a_2}\}$, resp. $v = \varepsilon$ if $Y = \emptyset$, using at most space $(\mathrm{size}(u, v_1, \mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k} \leq 2^{c \cdot \mathrm{size}(u, v_1, \mathcal{P})}$ for some constants $\bar{c}$, $c > 0$ independent of u, v_1, and $\mathcal{P}$.*

PROOF. We show that if there is a $v_2' \in [u]_\mathcal{P}$ with $v_2' = v_1 \cdot v \cdot w'$, where $w' \in (Y \cup Z)^\star$, then there is a $v_2 \in [u]_\mathcal{P}$ with the same properties and which can be determined in space $(\mathrm{size}(u, v_1, \mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k}$.

In addition to $x_1, \ldots, x_k$ we introduce three new variables s, $\bar{s}$, and t. Let $X_t = X \cup \{s, \bar{s}, t\}$. Given $\mathcal{P}$ and the two words u, $v_1 \in X^\star$, we construct a new commutative semigroup presentation $\mathcal{P}_t$ over X_t as follows. For every relation $l_i \equiv r_i$ in $\mathcal{P}$, $\mathcal{P}_t$ contains the relation $t \cdot l_i \equiv t \cdot r_i$. Then we add to $\mathcal{P}_t$ the relations $s \equiv t \cdot u$ and $t \cdot v_1 \cdot v \equiv \bar{s}$.
Let $\prec$ be any lexicographic term ordering satisfying

$$s \succ t \succ x \succ \bar{s} \succ y,$$

for all $x \in X - (Y \cup Z)$, $y \in Y \cup Z$.

By Theorem 3.2, $s \in LT(I(\mathcal{P}_t))$, and, since s is minimal in $LT(I(\mathcal{P}_t))$ w.r.t. divisibility, by Theorems 3.1 and 3.2, the binomial $s - m_s$, where m_s is the minimal element of $[s]_{\mathcal{P}_t}$ w.r.t. $\prec$, is an element of the reduced Gröbner basis of $I(\mathcal{P}_t)$ w.r.t. $\prec$.

We assume that there is a $v_2' \in [u]_\mathcal{P}$ such that $v_2' = v_1 \cdot v \cdot w'$ for some $w' \in (Y \cup Z)^\star$. Then we have $t \cdot v_1 \cdot v \cdot w' \in [t \cdot u]_{\mathcal{P}_t}$. As $t \cdot v_1 \cdot v \cdot w' \equiv \bar{s} \cdot w' \bmod \mathcal{P}_t$, we have $\bar{s} \cdot w' \in [t \cdot u]_{\mathcal{P}_t}$. Since m_s is the minimal element of $[s]_{\mathcal{P}_t} = [t \cdot u]_{\mathcal{P}_t}$, we also have $m_s \prec \bar{s} \cdot w'$ or $m_s = \bar{s} \cdot w'$. In particular, the variables s, t, and the variables in $X - (Y \cup Z)$ do not occur in m_s.

In $\mathcal{P}_t$ the variable s as well as the variable $\bar{s}$ occur in exactly one relation, namely $s \equiv t \cdot u$, resp. $t \cdot v_1 \cdot v \equiv \bar{s}$. In the remaining relations in $\mathcal{P}_t$ each side has the form $t \cdot y$ with $y \in X^\star$. Thus, the only relation in $\mathcal{P}_t$ that can be applied to s is $s \equiv t \cdot u$, and any derivation in $\mathcal{P}_t$ starting at s first leads from s to $t \cdot u$, i.e. $s \to t \cdot u(\mathcal{P}_t)$. Generally, from the structure of $\mathcal{P}_t$ we have the following result.

LEMMA 5.5. *Every word γ in a derivation in $\mathcal{P}_t$ starting at s satisfies*

$$\Phi(\gamma, s) + \Phi(\gamma, \bar{s}) + \Phi(\gamma, t) = 1.$$

Together with the above considerations, we get for the minimal element m_s (w.r.t. $\prec$) of $[s]_{\mathcal{P}_t}$ that $\Phi(m_s, \bar{s}) = 1$, i.e. $m_s = \bar{s} \cdot w$ for some $w \in (Y \cup Z)^\star$ with $w \prec w'$, or $w = w'$.

In the following it will be shown that in a repetition-free derivation in $\mathcal{P}_t$ leading from s to m_s the variables s and $\bar{s}$ only occur in the words s and m_s. Furthermore, we will see that, except for s and m_s, any word in a repetition-free derivation of m_s from s in $\mathcal{P}_t$ has the form $t \cdot x$ with $x \in X^\star$.

If some word γ_i, $i \in \mathbb{N}$, $i \geq 1$, in a derivation $s \to t \cdot u = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_{i-1} \to \gamma_i$ $(\mathcal{P}_t)$ contains the variable s, then the only way to continue is to apply the relation $s \equiv t \cdot u$, because this is the only relation of $\mathcal{P}_t$ in which s occurs. For the same reason γ_i must be derived from γ_{i-1} also by application of the relation $s \equiv t \cdot u$, causing a repetition in the resulting derivation.

Similarly, if some word γ in a derivation of m_s from s in $\mathcal{P}_t$ contains the variable

$\bar{s}$, then either $\gamma = m_s$ and we are finished, or there is exactly one applicable relation, namely the relation applied last, causing a repetition in the derivation.

Hence, the words γ_i in a repetition-free derivation

$$s \to t \cdot u = \gamma_0 \to \gamma_1 \to \cdots \to \gamma_{n-1} \to \gamma_n \to m_s(\mathcal{P}_t)$$

with $n \in \mathbb{N}$, do not contain s or $\bar{s}$. The only relations applied to γ_i, $i \in \{0, \ldots, n-1\}$ are the relations $t \cdot l_i \equiv t \cdot r_i$. Thus, any repetition-free derivation in $\mathcal{P}_t$ leading from s to m_s has the form

$$s \to t \cdot u \to t \cdot \delta_1 \to \cdots \to t \cdot \delta_n = t \cdot v_1 \cdot v \cdot w \to \bar{s} \cdot w = m_s(\mathcal{P}_t)$$

with $\delta_i \in X^\star$, $i \in I_n$, $n \in \mathbb{N}$.

We obtain the following derivation in $\mathcal{P}$ leading from u to $v_2 = v_1 \cdot v \cdot w$:

$$u \to \delta_1 \to \cdots \to \delta_n = v_1 \cdot v \cdot w = v_2(\mathcal{P}).$$

Since the binomial $s - m_s$ is an element of the reduced Gröbner basis of $I(\mathcal{P}_t)$, by Theorem 4.1, $m_s = \bar{s} \cdot w$ can be determined in space $(\text{size}(u, v_1, \mathcal{P}_t))^2 \cdot 2^{d \cdot k}$, and thus, v_2 can be determined using at most space $(\text{size}(u, v_1, \mathcal{P}))^2 \cdot 2^{\bar{c} \cdot k}$.□

As an example of Theorem 5.3, consider the finite commutative semigroup presentation $\mathcal{P} = \{x_1 \equiv x_2x_3, x_1 \equiv x_2x_3^3, x_2x_3^4 \equiv x_2\}$ over $X = \{x_1, x_2, x_3\}$, the words $u = x_1$, $v_1 = x_1$ and the sets $Y = \{x_3\}$, $Z = \emptyset$. In this special case the subword problem is to decide whether there is a $v_2 \in [x_1]_\mathcal{P}$ such that $v_2 = x_1x_3 \cdot w$ for some $w \in \{x_3\}^\star$.

Using the construction of Theorem 5.3 we compute the reduced Gröbner basis G of the ideal

$$I := \langle tx_1 - tx_2x_3, tx_1 - tx_2x_3^3, tx_2x_3^4 - tx_2, s - tx_1, tx_1x_3 - \bar{s} \rangle$$

w.r.t. the lexicographic term ordering $\succ$ satisfying

$$s \succ t \succ x_1 \succ x_2 \succ \bar{s} \succ x_3.$$

We obtain

$$G = \{\bar{s}x_3^2 - \bar{s}, \bar{s}x_1 - \bar{s}x_2x_3, tx_2 - \bar{s}, tx_1 - \bar{s}x_3, s - \bar{s}x_3\}.$$

The binomial $s - \bar{s}x_3$ provides the solution $w = x_3$, resp. $v_2 = x_1x_3^2$, which can be verified by the following derivation in $\mathcal{P}$:

$$u = x_1 \to x_2x_3 \to x_2x_3^5 \to x_1x_3^2 = v_2(\mathcal{P}).$$

THEOREM 5.4. *The subword problem for commutative semigroups is exponential space complete with respect to log–lin reducibility.*

PROOF. From the results in Mayr and Meyer (1982) we know that the word problem for commutative semigroups is exponential space complete with respect to log–lin reducibility. Since the word problem is a special case of the subword problem, and because of Theorem 5.3 we conclude the assertion.□

6. Conclusion

The results obtained in this paper first give an algorithm for generating the reduced Gröbner basis of a binomial ideal using at most space $2^{c \cdot n}$, where n is the size of the

problem instance, and $c > 0$ is some constant independent of n. Since, in the worst case, any Gröbner basis of a binomial ideal will have maximal degree double exponential in n, any algorithm for computing Gröbner bases of binomial ideals requires at least exponential space (see Mayr and Meyer, 1982; Huynh, 1986).

As an application of our basis construction algorithm, we also presented space optimal decision procedures for the finite enumeration and subword problems for commutative semigroups. These procedures also require at most space $2^{d \cdot n}$ for some constant d independent of the size n of the problem instance. This complexity bound for the finite enumeration problem also implies an analogous bound for the finite containment problem (FCP) (and the finite equality problem (FEP)) for commutative semigroups and, equivalently, for reversible Petri nets. For an investigation of the finite containment problem for general (not necessarily reversible) Petri nets see Mayr and Meyer (1981).

In view of commutative semigroups, we have also derived from the results reported in this paper an exponential space algorithm which, for a given word u of a commutative semigroup, constructs a closed representation of the congruence class $[u]$ as a uniformly semilinear set (see Koppenhagen and Mayr, 1997). For this algorithm, we first show that the minimal periods of $[u]$ can be determined requiring at most space $2^{c \cdot \text{size}(u,\mathcal{P})}$ for some constant $c > 0$ independent of u and $\mathcal{P}$, using the algorithm for the subword problem in commutative semigroups as reported here. Then we show an analogous bound for the minimal elements of $[u]$. We project $[u]$ onto its bounded coordinates and then again make use of the subword algorithm. The bounded coordinates can be found by an exponential space algorithm for the coverability problem.

References

Bayer, D. (1982). The division algorithm and the Hilbert scheme. Ph.D. Thesis, Harvard University, Cambridge, MA.

Buchberger, B. (1965). Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. Ph.D. Thesis, Department of Mathematics, University of Innsbruck.

Buchberger, B. (1983). A note on the complexity of computing Gröbner-bases. In *Proceedings of the European Computer Algebra Conference, Eurocal'83, New York*, LNCS **162**, pp. 137–145. London, U.K., Springer.

Caniglia, L., Galligo, A., Heintz, J. (1988). Some new effectivity bounds in computational geometry. In *Proceedings of the Sixth International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Rome, Italy*, LNCS **357**, pp. 131–151. Berlin, Springer.

Dickson, L. E. (1913). Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. *Am. J. Math.*, **35**, 413–422.

Dubé, T. W. (1990). The structure of polynomial ideals and Gröbner bases. *SIAM J. Comput.*, **19**, 750–773.

Eisenbud, D., Sturmfels, B. (1996). Binomial ideals. *Duke Math. J.*, **84**, 1–45.

Fortune, S., Wyllie, J. (1978). Parallelism in random access machines. In *Proceedings of the 10th Annual ACM Symposium on the Theory of Computing, San Diego, CA, U.S.A.*, pp. 114–118. New York, ACM Press.

Hermann, G. (1926). Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.*, **95**, 736–788.

Hironaka, H. (1964). Resolution of singularities of an algebraic variety over a field of characteristic zero: I. *Ann. Math.*, **79**, 109–203.

Huynh, D. T. (1986). A superexponential lower bound for Gröbner bases and Church–Rosser commutative Thue systems. *Inf. Control*, **68**, 196–206.

Koppenhagen, U., Mayr, E. W. (1995). The complexity of the boundedness, coverability, and selfcoverability problems for commutative semigroups. Technical Report TUM-I9518, Institut für Informatik, Technische Universität München.

Koppenhagen, U., Mayr, E. W. (1997). The complexity of the coverability, the containment, and the equivalence problems for commutative semigroups. In *Proceedings of the 11th International Symposium on Fundamentals of Computation Theory, Krakow, Poland, FCT'97*, LNCS **1279**, pp. 257–268. New York, Springer.

Krick, T., Logar, A. (1991). Membership problem, representation problem and the computation of the radical for one-dimensional ideals. In *Effective Methods in Algebraic Geometry (MEGA'90), Progress in Mathematics 94, Livomo, Italy*, pp. 203–216. Berlin, Birkhäuser.

Kühnle, K., Mayr, E. W. (1996). Exponential space computation of Gröbner bases. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC '96, Zurich*, New York, ACM Press.

Lazard, D. (1983). Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In *Proceedings of the European Computer Algebra Conference, Eurocal'83, London, U.K.*, LNCS **162**, pp. 146–156. New York, Springer.

Loos, R. (1982). Generalized polynomial remainder sequences. In Buchberger, B., Collins, G., Loos, R. eds, *Computer Algebra*, pp. 115–137. Wien-New York, Springer.

Mayr, E. W., Meyer, A. (1981). The complexity of the finite containment problem for Petri nets. *J. ACM*, **28**, 561–576.

Mayr, E. W., Meyer, A. (1982). The complexity of the word problems for commutative semigroups and polynomial ideals. *Adv. Math.*, **46**, 305–329.

Möller, H. M., Mora, F. (1984). Upper and lower bounds for the degree of Gröbner bases. In *Proceedings of the Third International Symposium on Symbolic and Algebraic Computation EUROSAM 84, Cambridge, U.K.*, LNCS **174**, pp. 172–183. Berlin, Springer.

Robbiano, L. (1985). Term orderings on the polynomial ring. In *Proceedings of the 10th European Conference on Computer Algebra, EUROCAL '85. Vol. 2: Research contributions Linz, Austria, April 1–3, 1985*, LNCS **204**, pp. 513–517. Berlin, Springer.

Weispfenning, V. (1987). Admissible orders and linear forms. *ACM SIGSAM Bull.*, **21**, 16–18.

Originally Received 3 July 1996
Accepted 27 May 1999